Oracle® Universal Content Management
Content Tracker Installation Guide
10*g* Release 3 (10.1.3.3.0)

May 2010

Content Tracker Installation Guide, 10*g* Release 3 (10.1.3.3.0)

Contributing Authors: Deanna Burke

Contributors: Evan Suits

Table of Contents

Chapter 3: Post-Installation

Chapter 4: Alternate Database Provider

Appendix A: Content Tracker Support for Content Server Configurations

Appendix B: Update Installations

Appendix C: Third Party Licenses

Chapter

1

INTRODUCTION

OVERVIEW

This section contains the following topics:

- ❖ About This Guide (page 1-1)
- ❖ What's New (page 1-3)
- ❖ Before You Begin (page 1-5)
- ❖ Pre-Installation Tasks and Considerations (page 1-9)
- ❖ Installation Overview (page 1-11)
- ❖ Software Requirements (page 1-12)
- ❖ Conventions (page 1-13)

ABOUT THIS GUIDE

This section contains the following topics:

- ❖ Component Overviews (page 1-2)
- ❖ Audience (page 1-3)

Component Overviews

Content Tracker and Content Tracker Reports are separate modules but work together to provide information about system usage. The information provided enables you to determine which content items are most frequently accessed and what content is most valuable to users or specific groups.

Understanding the consumption patterns of your organization's content is essential to successful content management. This enables you to provide more appropriate, user-centric information more effectively. This section summarizes both components:

- Content Tracker Overview (page 1-2)
- Content Tracker Reports Overview (page 1-2)

Content Tracker Overview

Content Tracker monitors your system and records information about various activities. This information is collected from various sources, then merged and written to a set of tables in your Content Server database. You can customize Content Tracker to change or expand the types of information it collects. Content Tracker monitors activity from:

- **Content Item Accesses:**

  Content Tracker gathers information about content item usage. The data is obtained from Web filter log files, the Content Server database, and other external applications such as portals and Web sites. Content item access data includes dates, times, content IDs, current metadata, user names, and profile information about users.

- **Content Server Services:**

  Content Tracker tracks all services that return content, as well as services that handle search requests. And, with a simple configuration change, Content Tracker can monitor any top-level service that is called via the server socket port, even custom services.

Content Tracker Reports Overview

After Content Tracker extracts data and populates applicable database repository tables, the information is available for report generation. Content Tracker Reports enables you to:

- **Generate Reports:**

  Content Tracker Reports queries the tables created by Content Tracker and generates summary reports of various kinds of activities and the usage history of particular content items. The reports help you analyze specific groups of content or users based on metadata, file extensions, or user profiles. You can use the pre-defined reports that are provided, customize them to suit your installation, or use a compatible third-party reporting package.

- **Optimize Content Management Practices:**

  You can also use the reported data for content retention management. That is, depending on the access frequency of particular content items during specific time intervals, you may decide to archive or delete some of the items. Similarly, applications can use the data to provide portlets with the top content for particular types of users.

Audience

This installation guide is intended for systems administrators who will be installing and configuring the Content Tracker and Content Tracker Reports components. This guide assumes that you are familiar with Oracle products and the architecture of Content Server.

WHAT'S NEW

This section describes the new features and enhancements in the 10gR3 versions of Content Tracker and Content Tracker Reports components. For more detailed information about any of these features, refer to the *Content Tracker Administration Guide*.

- **Custom Metadata Fields For Search Relevance Information:**

  The snapshot function enables you to link activity metrics to custom metadata fields that can be populated with content item usage information. The data gathered by the activity metrics includes the date of the most recent access and the number of accesses in two distinct time periods. You can use the collected data in various ways. For example, you might want to order search results according to the most popular or most viewed content in the last week.

- **Count Checkin Operations as Access Activity:**

  When a content item is checked in, the Last Access field in Content Server's DocMeta database table is initially empty. After a data reduction has been performed, the Last Access field is updated with the most recent date and time of access, or with the date and time of checkin if no accesses have occurred. An optional automatic load function allows you to update the last access activity metric for existing content to ensure that the Last Access field for content items is appropriately timestamped.

- **Greater Flexibility With Extended Service Logging:**

  The extended services logging function enables you to map and log data from most Content Server services to the combined output database table (SctAccessLog). This means that in addition to logging calls for services, you can now track specific data values that are relevant to those services.

- **Audit Trails for Failed User Authentications/Authorizations:**

  Content Tracker Reports now provides an auditing feature that enables you to monitor unsuccessful attempts to access the system or permission-protected content. Two reports are available that can help you analyze attempted security breaches that include failed user logons and unsuccessful attempts to access secure content items. This information is vital to ensure system and content security.

- **Filtered Report Results Based on User's Role/Account Permissions:**

  With this version of Content Tracker Reports, you can choose to generate reports in secure or non-secure mode. That is, you now have the option to filter the search results in reports based on the requesting user's role and account permissions. The same criteria that are used to limit Content Server search results can be used to restrict the content items that are included in the generated reports.

- **Include Both External and Internal User Access Data in Reports:**

  With this version of Content Tracker and Content Tracker Reports, the role and account information for externally authenticated users is recorded in the Content Server's UserSecurityAttributes database table. As a result, two pre-defined reports (Top Content Items by User Role and Users by User Role) include the content item access activity by external users.

- **DataBinder Dump Facility to Debug Field Maps for Extended Service Logging:**

  If you plan to use the extended service logging function, the DataBinder dump facility is available to help you design and debug the field maps. This facility allows Content Tracker to write the DataBinder objects to a dump file and enables you to see what data is available when service events are recorded.

- **Web Site Access Activity (Site Studio):**

  With this version, there are pre-defined reports that you can use to generate and analyze Site Studio-specific data. One report summarizes content accesses from web site pages. Another report summarizes web site page visits.

- **Localization Support:**

  This version of Content Tracker and Content Tracker Reports provides localized translations for the components' user interfaces and error messages. The supported languages include German, French, Spanish, Brazilian Portuguese, Dutch, Japanese, and Korean.

Before You Begin

This section covers the following topics:

- Sybase Database Issues (page 1-5)
- DB2 Database Issues (page 1-6)
- Oracle Database Issue (page 1-7)
- HP-UX Operating System Issue (page 1-7)
- HP-UX Operating System Issue (page 1-7)
- Access Control Lists and Content Tracker Reports Secure Mode (page 1-7)
- Master/Proxy Installations (page 1-8)

Sybase Database Issues

This section provides information that is pertinent to users who are:

- Running Content Tracker in combination with a Sybase database and are planning to install Content Tracker 10gR3.

Known Sybase database issues include:

- **Primary Keys:**

  Primary keys have been added to all of the Sct tables (reduction data sets). For more detailed information about the Sct tables (reduction data sets), refer to the *Content Tracker Administration Guide*.

- **Logical Page Size:**

  Logical page size limits the total number of characters that a table row can contain. When running Content Tracker on Sybase, the recommended maximum logical page size is 16KB. This ensures that Content Tracker will work properly.

- **Case Sensitivity and Sort Order Setting:**

  When running Content Tracker on Sybase, there are case sensitivity issues that affect search keys in SELECT statements. To resolve these case sensitivity problems, Sybase database users must ensure that their database sort order is not case sensitive. Case sensitivity for the sort order is a server-wide setting, related to language and character sets, that is configured with a platform-dependent utility—ServerConfig in Windows and the equivalent in UNIX.

  If this case-sensitivity setting must be revised, users must also re-index the Content Server database after changing the setting value. If the database is not re-indexed immediately after the setting is changed, Sybase will issue applicable warnings the next time. The re-indexing process must be performed using the DBCC REINDEX function.

DB2 Database Issues

If you are using DB2 as your Content Server database, you will need to make some configuration changes. DB2 database issues include:

- **Tablespace Pagesize:**

  You will need to configure the tablespace to use a larger pagesize before you install Content Tracker. Because DB2 has a default pagesize of 4 KB, Content Tracker will not be able to create the SctAccessLog table during installation. The pagesize must be increased to 32 KB. See Configuring the Tablespace to Use 32 KB Pagesize (DB2 Only) (page 2-2).

Important: Content Tracker does not work with IBM DB2 as an alternate database provider. Therefore, the default SystemDatabase provider must be used. For more information about specifying an alternate database provider, see Chapter 4 (*Alternate Database Provider)*.

- **Primary Keys:**

  You will need to include a variable in Content Server’s config.cfg file to support the lengths of DB2 primary key names. Content Server normally creates tables with unrestricted lengths for primary key names in tables. The DB2 server, however, has an

18-character limit on the lengths of key names. When you add the key length configuration variable to the config.cfg file, it instructs Content Server to use abbreviated key names. See Configuring Content Server to use Abbreviated Key Names (DB2 Only) (page 2-3).

Oracle Database Issue

Content Tracker's SctAccessLog table has three columns that are used to store URLs. Each column has a default length of 3000 characters. For normal character sets, this is not a problem. However, Oracle NVARCHAR fields are restricted to 4000 bytes and Unicode characters occupy two bytes each.

Therefore, if you are using an Oracle database and have it configured for Unicode, then the maximum field size is 2000 characters (4000 bytes). To accommodate this, when you install Content Tracker, you will need to set the maximum number of characters for URL length to 2000 (the default is 3000).

To set the maximum number of characters for the URL length, see step 7f for Installing the Content Tracker Component using Component Manager (page 2-5) or step 7f for Installing the Content Tracker Component using Component Wizard (page 2-8).

HP-UX Operating System Issue

If you have installed Content Tracker on an HP-UX operating system, Content Tracker will not automatically collect data in the data/ directory. To ensure proper data collection, you must manually give execution permission to the HP-UX web server filter. See Grant Execution Permission to the Web Server Filter (HP-UX Only) (page 3-2).

Access Control Lists and Content Tracker Reports Secure Mode

The security checks preference variable (SctrEnableSecurityChecks) is set when you install the Content Tracker Reports component. Essentially, this preference variable enables you to select one of two security modes: secure and non-secure. The security checks preference provides the option to employ individual user role and account information to restrict the visibility of content item information in report results.

This means that you control what content items (and, subsequently, the metadata) that users can see in their generated reports. Ideally, users should not be able to see anything through Content Tracker Reports that they couldn't find via a Content Server search. Therefore, if you select the secure mode, the information in any generated report will be filtered based on the user’s role and account privileges.

However, if you have enabled Access Control Lists (ACLs) on your Content Server instance, the secure mode option in Content Tracker Reports does not work. During installation, you must leave the security checks preference check box blank. This means that on an ACL-based system, the secure mode must be disabled. In this case, it is possible for users other than a system administrator to see information about content items that they would not otherwise be authorized to access and view.

Note: For specific information about the installation preference prompt and the two security checks options, see Instructions for Content Tracker Reports New Install (page 2-13). For more detailed information about the security checks installation preference and how it will affect the report queries and report results, refer to the *Content Tracker Administration Guide*.

Master/Proxy Installations

Content Tracker is fully supported for installation and use on configurations that include both Master and Proxy Content Servers. However, before you install Content Tracker on any Proxy server, you must first have installed it on the associated Master server. Also, the recommended use in such situations is that Content Tracker be installed on all Proxy servers associated with a given Master. This is because Content Tracker determines the group membership and account properties of a user by connecting to the primary server for that user (that is, the server on which the user account is defined).

Therefore, if you have Content Tracker installed on the Master server but not on one or more of the Proxy servers, and if a Proxy user logs onto or otherwise interacts with the Master server, Content Tracker will attempt to contact the user’s Proxy server during the next reduction run. If Content Tracker is not installed on the Proxy server, the connection attempt will fail and a diagnostic message will be included in the reduction log.

Pre-Installation Tasks and Considerations

Before starting the installation process, the following pre-installation tasks and considerations should be taken into account:

- ❑ If you are using a Sybase database, make sure that the case-sensitivity setting has the correct value. If the setting must be revised, re-index your database after changing the setting. See Case Sensitivity and Sort Order Setting: (page 1-6).
- ❑ If you are using Sybase as your Content Server database, make sure that the logical page size is 16KB. See Logical Page Size: (page 1-6).
- ❑ If you are using DB2 as your Content Server database, make sure you increase the pagesize from the default of 4 KB to 32 KB before you install Content Tracker. Otherwise, Content Tracker will not be able to create the SctAccessLog table during installation. See Configuring the Tablespace to Use 32 KB Pagesize (DB2 Only) (page 2-2).
- ❑ If you are using DB2 as your Content Server database, make sure you configure Content Server to use abbreviated key names. See Configuring Content Server to use Abbreviated Key Names (DB2 Only) (page 2-3).
- ❑ Ensure that the metadata field structure for your system is complete.

Note: We recommend that you establish your metadata structure before installing Content Tracker. For more detailed information about metadata models, refer to the *Content Server Implementation and Planning Guide* and *Content Server Getting Started Guide*.

- ❑ Save any files, tables, and directories that contain data you want to retain.
- ❑ Determine the maximum number of characters for the URL length. You will be prompted to provide this information during the Content Tracker installation process. The default value is 3000 characters.
- ❑ If you are using Oracle as your Content Server database and have it configured for Unicode, you will need to limit the size of the maximum number of characters for the URL length. Oracle VARCHAR2 and NVARCHAR2 column names are restricted to 4000 bytes which limits unicode fields to 2000 characters. If you are using UTF-8 (AL32URT8) encoding on the Content Server, then the field size should be limited to 1333 characters. See Oracle Database Issue (page 1-7).
- ❑ Determine the maximum number of characters for the Content Server proxy instance name. You will be prompted to provide this information during the Content Tracker installation process. The default value for the proxy instance name is 50 characters.

- ❑ Determine the number of the data collection synchronization lock port. You will be prompted to provide this port number during the Content Tracker installation process. The default value for this port is 4477.
- ❑ If you plan to provide an optional executable file to run after data reduction is completed, determine and note the filename of this executable. You will be prompted to enter the name of this executable during the Content Tracker installation process for a new install [see Instructions for Content Tracker New Install (page 2-5) and Post-Reduction Executable Set Up (page 3-3)].
- ❑ If you plan to use Content Tracker in a cluster configuration, the installation preference settings may require values other than the defaults. Be prepared to provide the proper values when prompted for these settings during the Content Tracker installation process. See Installing Content Tracker in a Multi-Node Cluster Configuration (page 2-11) and Configuring Content Tracker for Cluster Installations (page A-8).
- ❑ Decide whether you want to restrict the visibility of content item information in report results. You will be prompted to enable or disable the security checks preference variable during the Content Tracker Reports installation process. For more detailed information about this variable, refer to the *Content Tracker Administration Guide*.

Caution: If you have enabled Access Control Lists (ACLs) on your Content Server instance, the secure mode option in Content Tracker Reports does not work. For more information, see Access Control Lists and Content Tracker Reports Secure Mode (page 1-7).

- ❑ If you plan to use Site Studio, you must install the correct version (Site Studio 10gR3) to ensure compatibility with the Content Tracker and Content Tracker Reports components. After Site Studio 10gR3 is installed, the pre-defined Web site access reports are displayed.

INSTALLATION OVERVIEW

Chapter 2 (*Installation)* provides the procedures for the actual installation of the Content Tracker and Content Tracker Reports components. These include:

- Installing Content Server (page 2-1)

  This section briefly describes the Content Server installation process and includes important notes and tasks applicable for certain databases. It also provides references to other installation documents that contain more detailed instructions.

- Installing Site Studio (page 2-4)

  If you are using Site Studio, this section briefly describes the installation process and includes important notes and references to other installation documents that contain more detailed instructions.

- Installing Content Tracker (page 2-5)

  This section provides detailed, step-by-step installation instructions for both update and new Content Tracker installs. For your convenience, this section includes both Component Manager and Component Wizard installation procedures.

- Installing Content Tracker in a Multi-Node Cluster Configuration (page 2-11)

  If you are planning to install Content Tracker in a cluster configuration, some of the steps in the standard Content Tracker installation procedure require various changes to support the cluster architecture. This section provides that information.

  After installation, Content Tracker requires some additional, cluster-specific configurations. The section on Configuring Content Tracker for Cluster Installations (page A-8) provides the detailed, step-by-step configuration instructions.

- Installing Content Tracker Reports (page 2-12)

  This section provides detailed, step-by-step installation instructions for both update and new Content Tracker Reports installs. For your convenience, this section includes both Component Manager and Component Wizard installation procedures.

- Restart Cycle for Master/Proxy Installations (page 2-16)

  If you are using a master/proxy Content Server configuration, some additional steps are necessary to complete the Content Tracker install. This section provides that information. For related consideration and requirement information, see Master/Proxy Installations (page 1-8).

SOFTWARE REQUIREMENTS

This section contains the following topics:

Compatibility with Content Server

Currently, the 10gR3 versions of Content Tracker and Content Tracker Reports are supported on Content Server version 10gR3.

Operating Systems

The current version of Content Tracker supports the following operating systems:

- Windows 2000 Server with Service Pack 4
- Windows Server 2003, Web Edition
- Windows Server 2003, Standard Edition
- Windows Server 2003, Enterprise Edition (32-bit)
- HP-UX 11i v2
- Sun Solaris 9, 10
- IBM AIX 5.2 or 5.3
- Linux SuSe 9 SP2
- Linux Red Hat Enterprise ES3, ES4, AS3, AS4

Web Servers

The current version of Content Tracker supports the following web servers:

- Microsoft Internet Information Services (IIS) 5.0 or 6.0
- SunONE 6.1 with latest service packs
- IBM HTTP Server 2.0.42 (IBM AIX only), 6.02

- Apache 2.0.55 or higher
- Apache 2.2 (for UNIX only)

Databases

The current version of Content Tracker supports the following databases:

- Microsoft SQL Server 2000 with Service Pack 4
- Oracle Database 9.2.0.8 or 10gRAC, 10gR2
- IBM DB2 8.1, 8.2
- Sybase Adaptive Enterprise Server 15

CONVENTIONS

The following conventions are used throughout this guide:

- The notation *<Install_Dir>/* is used to refer to the location on your system where the Content Server instance is installed.
- Forward slashes (/) are used to separate the directory levels in a path name. A forward slash will always appear after the end of a directory name.
- Notes, technical tips, important notices, and cautions use these conventions:

Symbols	**Description**
💡	This is a note. It is used to bring special attention to information.
⚙	This is a technical tip. It is used to identify information that can be used to make your tasks easier.
❗	This is an important notice. It is used to identify a required step or required information.
✖	This is a caution. It is used to identify information that might cause loss of data or serious system problems.

Chapter

2

INSTALLATION

OVERVIEW

This section covers the following topics:

- Installing Content Server (page 2-1)
- Installing Site Studio (page 2-4)
- Installing Content Tracker (page 2-5)
- Installing Content Tracker in a Multi-Node Cluster Configuration (page 2-11)
- Installing Content Tracker Reports (page 2-12)
- Restart Cycle for Master/Proxy Installations (page 2-16)

INSTALLING CONTENT SERVER

Install Content Server 7.5.2 or 10gR3 before installing Content Tracker. If you are updating your software to a new version of Content Server, please read Configuring the Tablespace to Use 32 KB Pagesize (DB2 Only) (page 2-2) that follows.

Important: If you are using DB2 as your Content Server database, you will need to configure the tablespace to use a larger pagesize before you install Content Tracker. Because DB2 has a default pagesize of 4 KB, Content Tracker will not be able to create the SctAccessLog table during installation. See Configuring the Tablespace to Use 32 KB Pagesize (DB2 Only) (page 2-2).

Important: If you are using DB2 as your Content Server database, you will need to configure Content Server to use abbreviated primary key names for table columns. See Configuring Content Server to use Abbreviated Key Names (DB2 Only) (page 2-3).

1. Refer to the *Content Server Installation Guide for Microsoft Windows* or *Content Server Installation Guide for UNIX*.
2. Install the content server software.

Configuring the Tablespace to Use 32 KB Pagesize (DB2 Only)

DB2 has a default pagesize of 4 KB. With this size, Content Tracker cannot create the SctAccessLog table during the installation process. To correct this, the pagesize must be increased to 32 KB as follows:

1. Using a DB2 command line processor, enter the following lines to create a BufferPool that has a 32 KB page size:

```
CONNECT TO <db_name> USER <user_name> USING <password>

CREATE BUFFERPOOL WIDE SIZE 250 PAGESIZE 32k

DISCONNECT <db_name>
```

Note: If you have more than one database in the current DB2 instance, you must find the applications that are using the database specified in step 1 of this procedure. Proceed to the next step.

Otherwise, if you do not have applications using the specified database, proceed to step 4 of this procedure.

2. To find the applications, enter the following command:

```
LIST APPLICATIONS FOR DATABASE <db_name>
```

3. To close the applications found in step 2 of this procedure, enter the following command:

```
FORCE APPLICATION <application-handle>
```

4. Enter the following lines to force the database reload to activate the newly created BufferPool:

```
FORCE APPLICATION ALL

DEACTIVATE DATABASE <db_name>

ACTIVATE DATABASE <db_name>
```

Note: If any of these three command lines does not return DB20000I, finish all three commands and then run them again.

5. Enter the following lines to create tablespace and temporary tablespace:

```
CONNECT TO <db_name> USER <user_name> USING <password>

CREATE TABLESPACE WIDE_TBSP PAGESIZE 32K MANAGED BY SYSTEM USING
('<absolute_directory_path_for_this_tablespace>') BufferPool WIDE

CREATE TEMPORARY TABLESPACE TEMP_WIDE_TBSP PAGESIZE 32K MANAGED BY
SYSTEM USING ('<absolute_directory_path_for_this_temp_tablespace>')
BufferPool WIDE

DISCONNECT <db_name>
```

Note: Make sure the user_name and password used in this step conform with the JdbcUser and JdbcPassword. Otherwise, you will need to grant access rights to JdbcUser on these newly created tablespaces.

6. Enter the following lines to drop the default tablespace:

Note: Before running the following commands, make sure there are no tables in the default tablespace. Contact your database administrator if you are unsure. Otherwise the following commands may result in data loss.

```
CONNECT TO <db_name> USER <user_name> USING <password>

DROP TABLESPACE USERSPACE1

DISCONNECT <db_name>
```

Configuring Content Server to use Abbreviated Key Names (DB2 Only)

You will need to include a variable in Content Server’s config.cfg file to support the length sizes of DB2 primary key names. Content Server normally creates tables with unrestricted lengths for primary key names in tables. The DB2 server, however, has an 18-character limit on the lengths of key names. When you add the key length configuration variable to the config.cfg file, it instructs Content Server to use abbreviated key names.

To ensure that Content Server uses abbreviated key names:

1. In a text editor, open the config.cfg file:

   <*install_dir*>/config/config.cfg

2. Add the following configuration variable:

   ```
   UseDatabaseShortIndexName=true
   ```

3. save and close the config.cfg file.
4. Restart Content Server to apply the changes.

INSTALLING SITE STUDIO

If you plan to use Site Studio, you must install the correct version (Site Studio 10gR3) to ensure compatibility with the Content Tracker and Content Tracker Reports components. After Site Studio 10gR3 is installed, the pre-defined Web site access reports are displayed. It is irrelevant whether you install Site Studio before or after you install Content Tracker and Content Tracker Reports. Upon detecting that Site Studio is installed, Content Tracker is configured to automatically track Site Studio activity including content accesses and node navigation.

Content Tracker Reports 10gR3 includes two pre-defined reports that provide statistics about Site Studio user activity. One report shows how Site Studio content is being accessed and where users are requesting content items. A second report shows how users are navigating through the Web site.

However, the reports are only displayed on the Content Tracker Report Generator main page when:

- Site Studio 10gR3 is installed
- Content Tracker is restarted
- Content Tracker Reports is accessed

To enable user activity tracking for Site Studio and activate the pre-defined reports:

1. Refer to the *Site Studio Installation Guide*.
2. Install the Site Studio software.

INSTALLING CONTENT TRACKER

This section includes step-by-step instructions for installing Content Tracker 10gR3:

- To perform a new installation of Content Tracker, see Instructions for Content Tracker New Install (page 2-5).

Instructions for Content Tracker New Install

Note: Content Tracker 10gR3 may be installed into a master or proxied instance of Content Server; however, the component must be installed in the master instance before it can be installed into a proxied instance.

You can install the Content Tracker component using either of the following methods:

- Installing the Content Tracker Component using Component Manager (page 2-5)
- Installing the Content Tracker Component using Component Wizard (page 2-8)

Installing the Content Tracker Component using Component Manager

Caution: Do not install Content Tracker on top of a previous version of Content Tracker. You must uninstall the old version of Content Tracker before you install the new version of Content Tracker.

To install the Content Tracker component using Component Manager:

1. Click the **Admin Server** applet icon on the Administration page.
2. Click the applicable Content Server instance button.
3. Click the **Component Manager** link.

   The Component Manager page is displayed.
4. Click **Browse**, navigate to the *ContentTracker.zip* file, select it, and click **Open**.

   The path is displayed in the Install New Component field.
5. Click **Install**.

   A list of component items that will be installed is displayed.
6. Click **Continue**.

The Install Settings dialog is displayed.

Caution: If you are planning to use Content Tracker in a cluster configuration, DO NOT continue to the next step. See Installing Content Tracker in a Multi-Node Cluster Configuration (page 2-11) to continue the Content Tracker installation process

7. Enter the appropriate information in the fields listed on the Install Settings dialog:
   a. **Track Content Access Only:** Default value is TRUE (a selected check box). This setting limits Content Tracker to gathering event information for content access requests. Information about searches, logins, and user data (groups, roles, and so forth) is *not* collected. In addition, the Services tab on the Content Tracker Applet Admin screen is hidden. If set to FALSE, then gathered information is not limited.
   b. **Do Not Populate Access Log Columns:** Default is string of non-essential SctAccessLog column names. This setting limits the amount of data that goes into the SctAccessLog table, thereby reducing storage requirements for the table. Columns named in the string are left empty.
   c. **Simply User Agent String:** Default value is TRUE (a selected check box). Content Tracker examines the HTTP_USER_AGENT field, and if it contains “java:” then whatever information follows is stored. If the field does not contain “java:” then Content Tracker stores “browser” information. If set to FALSE, then previous Content Tracker behavior is implemented.
   d. **Maximum Days to Retain Data:** Default value is 60. Retains database records for the specified number of days before they are considered “expired” and moved from the main Content Tracker tables to their Archive counterparts. This also helps to limit the storage requirements of the SctAccessLog table. See the “Do Not Archive Expired Data” setting.
   e. **Do Not Archive Expired Data:** Default is TRUE (a selected check box). Records that have “expired” are simply deleted from their tables. Prior versions of Content Tracker would move “expired” records from the various Sct tables to their Archive counterparts, which added overhead and could cause excessive storage requirements. See the “Maximum Days to Retain Data” setting.
   f. **Enter Maximum URL Length:** Default value is 3000 characters. This setting specifies the maximum number of characters for a URL.

Caution: If you are using Oracle as your Content Server database, and you are using Unicode string data types, you must set the maximum URL length preference value to 2000 at most. This is because the Oracle datatypes VARCHAR2 and NVARCHAR2 are restricted to 4000 bytes which limits unicode fields to 2000 characters. If you are using UTF-8 (AL32URT8) encoding on the Content Server, then the field size should be limited to 1333 characters. This ensures compatibility with the URL columns in Content Tracker's SctAccessLog database table.

Caution: If you are using Informix as your Content Server database, you must set the maximum URL length preference value to 255. This is because Informix does not support VARCHAR fields larger than 255 characters. Therefore, the default setting for the Max URL Size (3000) is unworkable.

g. **Enter Maximum Proxy Name Length:** Default value is 50 characters. This setting specifies the maximum number of characters for the name of the Content Server proxy instance.

h. **Enter Lock Port:** Default value is 4477. This settings specifies the data collection synchronization lock port number.

Note: When Content Tracker collects information about Content Server requests, it must synchronize access to its data files so that only one set of request information is written to a file at a time. This is managed through a locking mechanism, that uses an IP port number. The installer program presents a default port number, which may be accepted, or you may enter another unused port number. A different port number should be used for each instance (master or proxied) in which Content Tracker is installed.

i. **Post Reduction Executable:** (Optional) Enter the name of an executable to run after data reduction.

Note: After Content Tracker is completely installed, the executable should be manually copied into <*install_dir*>/custom/ContentTracker/bin/. For more information, see Post-Reduction Executable Set Up (page 3-3).

8. Click **Continue**.

   Component Manager asks if you want to immediately enable Content Tracker or return to the Component Manager. Select the option to enable Content Tracker.

Caution: If you plan to use Content Tracker in a cluster configuration, DO NOT restart Content Tracker after you have exited the Component Wizard. To complete the Content Tracker installation and configuration process for a cluster installation, see Configuring Content Tracker for Cluster Installations (page A-8).

9. Restart Content Server to apply the updated installation parameters.
10. Restart the web server and then restart Content Server once more to force a filter plugin reload with the updated installation parameters.

    The Content Tracker icon is available from the Content Tracker Administration page.

Installing the Content Tracker Component using Component Wizard

Caution: Do not install Content Tracker on top of a previous version of Content Tracker. You must uninstall the old version of Content Tracker before you install the new version of Content Tracker.

To install the Content Tracker component using Component Wizard:

1. Start the Component Wizard by selecting **Start—All Programs—Content Server—<*instance*>—Utilities—Component Wizard** (Windows) or by running the *ComponentWizard* script in the */bin* directory (UNIX).

   The Component Wizard main screen and the Component List screen are displayed.
2. On the Component List screen, click **Install**.

   The Install screen is displayed.
3. Click **Select**.

   The Zip File Path screen is displayed.
4. Navigate to the *ContentTracker.zip* file and select it.
5. Click **Open**.

   The zip file contents that will be installed are added to the Install screen list.
6. Click **OK**.

   The Edit Preference Prompt dialog is displayed.

Caution: If you are planning to use Content Tracker in a cluster configuration, DO NOT continue to the next step. See Installing Content Tracker in a Multi-Node Cluster Configuration (page 2-11) to continue the Content Tracker installation process.

7. Enter the appropriate information in the fields listed on the Edit Preference Prompt dialog:
   a. **Track Content Access Only:** Default value is TRUE (a selected check box). This setting limits Content Tracker to gathering event information for content access

requests. Information about searches, logins, and user data (groups, roles, and so forth) is *not* collected. In addition, the Services tab on the Content Tracker Applet Admin screen is hidden. If set to FALSE, then gathered information is not limited.

b. **Do Not Populate Access Log Columns:** Default is string of non-essential SctAccessLog column names. This setting limits the amount of data that goes into the SctAccessLog table, thereby reducing storage requirements for the table. Columns named in the string are left empty.

c. **Simply User Agent String:** Default value is TRUE (a selected check box). Content Tracker examines the HTTP_USER_AGENT field, and if it contains "java:" then whatever information follows is stored. If the field does not contain "java:" then Content Tracker stores "browser" information. If set to FALSE, then previous Content Tracker behavior is implemented.

d. **Maximum Days to Retain Data:** Default value is 60. Retains database records for the specified number of days before they are considered "expired" and moved from the main Content Tracker tables to their Archive counterparts. This also helps to limit the storage requirements of the SctAccessLog table. See the "Do Not Archive Expired Data" setting.

e. **Do Not Archive Expired Data:** Default is TRUE (a selected check box). Records that have "expired" are simply deleted from their tables. Prior versions of Content Tracker would move "expired" records from the various Sct tables to their Archive counterparts, which added overhead and could cause excessive storage requirements. See the "Maximum Days to Retain Data" setting.

f. **Enter Maximum URL Length:** Default value is 3000 characters. This setting specifies the maximum number of characters for a URL.

Caution: If you are using Oracle as your Content Server database, and you are using Unicode string data types, you must set the maximum URL length preference value to 2000 at most. This is because the Oracle datatypes VARCHAR2 and NVARCHAR2 are restricted to 4000 bytes which limits unicode fields to 2000 characters. If you are using UTF-8 (AL32URT8) encoding on the Content Server, then the field size should be limited to 1333 characters. This ensures compatibility with the URL columns in Content Tracker's SctAccessLog database table.

Caution: If you are using Informix as your Content Server database, you must set the maximum URL length preference value to 255. This is because Informix does not support VARCHAR fields larger than 255 characters. Therefore, the default setting for the Max URL Size (3000) is unworkable.

g. **Enter Maximum Proxy Name Length:** Default value is 50 characters. This setting specifies the maximum number of characters for the name of the Content Server proxy instance.

h. **Enter Lock Port:** Default value is 4477. This settings specifies the data collection synchronization lock port number.

Note: When Content Tracker collects information about Content Server requests, it must synchronize access to its data files so that only one set of request information is written to a file at a time. This is managed through a locking mechanism, that uses an IP port number. The installer program presents a default port number, which may be accepted, or you may enter another unused port number. A different port number should be used for each instance (master or proxied) in which Content Tracker is installed.

i. **Post Reduction Executable:** (Optional) Enter the name of an executable to run after data reduction.

Note: After Content Tracker is completely installed, the executable should be manually copied into <*install_dir*>/custom/ContentTracker/bin/. For more information, see Post-Reduction Executable Set Up (page 3-3).

8. Click **OK**.

   Component Wizard asks if you want to enable the Content Tracker component.

9. Click **Yes**.

   The Content Tracker component is listed as enabled on the Component List screen.

10. Exit the Component Wizard.

Caution: If you plan to use Content Tracker in a cluster configuration, DO NOT restart Content Tracker after you have exited the Component Wizard. To complete the Content Tracker installation and configuration process for a cluster installation, see Configuring Content Tracker for Cluster Installations (page A-8).

11. Restart Content Server to apply the updated installation parameters.

12. Restart the web server and then restart Content Server once more to force a filter plugin reload with the updated installation parameters.

    The Content Tracker icon is available from the Content Tracker Administration page.

INSTALLING CONTENT TRACKER IN A MULTI-NODE CLUSTER CONFIGURATION

If you are using Content Tracker in a cluster configuration, you will need to perform some manual configurations after the Content Tracker component is installed. Prepare Content Tracker for a cluster configuration, install and configure the component as follows:

1. Follow the instructions for a new Content Tracker install:

   Component Manager Installation:

   a. Perform steps 1 through 6 in the procedure for Installing the Content Tracker Component using Component Manager (page 2-5).

   b. In step 7, enter the following values for the installation preferences listed on the Install Settings dialog:

      - Maximum URL Length = 2000 (enter 3000 if you are NOT using Oracle UTF-8/UTF-16)
      - Maximum Proxy Name Length = 50 (default value)
      - Lock Port = 4477 (default value)
      - Post Reduction Executable = blank (default value)

   c. Click **Continue**. (As instructed in step 8.)

   d. Restart Content Server to apply the updated installation parameters.

   e. Restart the web server and Content Server once more to force a filter plugin reload with the updated installation parameters.

   Component Wizard Installation:

   a. Perform steps 1 through 6 in the procedure for Installing the Content Tracker Component using Component Wizard (page 2-8).

   b. In step 7, enter the following values for the installation preferences listed on the Edit Preference Prompt dialog:

      - Maximum URL Length = 2000 (enter 3000 if you are NOT using Oracle UTF-8/UTF-16)
      - Maximum Proxy Name Length = 50 (default value)
      - Lock Port = 4477 (default value)
      - Post Reduction Executable = blank (default value)

   c. Complete steps 8 through 10.

   d. Restart Content Server to apply the updated installation parameters.
   e. Restart the web server and Content Server once more to force a filter plugin reload with the updated installation parameters.

2. Manually configure Content Tracker for a cluster configuration. Perform the procedures provided in Configuring Content Tracker for Cluster Installations (page A-8).

INSTALLING CONTENT TRACKER REPORTS

The Content Tracker Reports component provides pre-defined report categories that include document usage reports, user access reports, and admin reports. Each category offers various query selections that extract applicable data from the data files or tables and generate the selected reports from the search results. Content Tracker Reports can be customized to add other queries or remove existing ones.

Content Tracker automatically uses the default Content Server database provider and subsequently creates the Sct user metadata tables in the Content Server database. For more detailed information about these tables, refer to the *Content Tracker Administration Guide*.

Important: Optionally, you can define an alternate database provider that points to an alternate database and the reduced data files (replicated). Although Content Tracker Reports supports the use of alternate database providers, you are responsible for making sure that the necessary Content Server database tables are replicated to the alternate database. For general instructions on defining an alternate database provider, see Chapter 4 *(Alternate Database Provider)*.

For step-by-step instructions to update or install Content Tracker Reports, use the installation procedure—update or new—that is appropriate to your situation:

❖ To perform a new installation of Content Tracker Reports, see Instructions for Content Tracker Reports New Install (page 2-13).

Instructions for Content Tracker Reports New Install

You can install the Content Tracker Reports component using either of the following methods:

- Installing the Content Tracker Reports Component using Component Manager (page 2-13)
- Installing the Content Tracker Reports Component using Component Wizard (page 2-15)

Installing the Content Tracker Reports Component using Component Manager

To install the Content Tracker Reports component using Component Manager:

1. Click the **Admin Server** applet icon on the Administration page.
2. Click the applicable Content Server instance button.
3. Click the **Component Manager** link.

   The Component Manager page is displayed.
4. Click **Browse**, navigate to the *ContentTrackerReports.zip* file, select it, and click **Open**.

   The path is displayed in the Install New Component field.
5. Click **Install**.

   A list of component items that will be installed is displayed.
6. Click **Continue**.

   The Install Settings dialog is displayed and provides a checkbox option for the Security Checks on Queries.

   - Selecting the checkbox enables the security checks installation preference and configures Content Tracker Reports to operate in secure mode.

     In secure mode, the same security criteria (role and account qualifications) that are used to limit Content Server search results for a particular user are also applied to the Content Tracker Report component’s queries and the generated reports. Thus, it is possible that two different users running the Top Content Items report may see different results.

❖ Leaving the checkbox blank (the default value) disables the security checks installation preference and configures Content Tracker Reports to operate in non-secure mode. This is the default setting.

In non-secure mode, the additional role and account criteria used to restrict Content Server search results for a particular user are not applied to Content Tracker Report component's queries and the generated reports. Thus, it is possible for a user other than a system administrator to see information about content items that they would not be authorized to access and view.

Caution: If you have enabled Access Control Lists (ACLs) on your Content Server instance, the secure mode option in Content Tracker Reports does not work. For more information, see Access Control Lists and Content Tracker Reports Secure Mode (page 1-7).

Note: For more detailed information about the security checks installation preference and how it will affect the report queries and report results, refer to the *Content Tracker Administration Guide*.

7. Select the security checks installation preference checkbox or leave it blank.
8. Click **Continue**.

   Component Manager asks if you want to immediately enable Content Tracker Reports or return to the Component Manager. Select the option to enable Content Tracker Reports.
9. Restart Content Server to apply the updated installation parameter.

   The Content Tracker Reports link is displayed in the Administration tray.

Installing the Content Tracker Reports Component using Component Wizard

To install the Content Tracker Reports component using Component Wizard:

1. Start the Component Wizard by selecting **Start—All Programs—Content Server—<*instance*>—Utilities—Component Wizard** (Windows) or by running the *ComponentWizard* script in the */bin* directory (UNIX).

   The Component Wizard main screen and the Component List screen are displayed.

2. On the Component List screen, click **Install**.

   The Install screen is displayed.

3. Click **Select**.

   The Zip File Path screen is displayed.

4. Navigate to the *ContentTrackerReports.zip* file and select it.

5. Click **Open**.

   The zip file contents that will be installed are added to the Install screen list.

6. Click **OK**.

   The Edit Preference Prompt dialog is displayed and provides a checkbox option for the Security Checks on Queries.

   - ❖ Selecting the checkbox enables the security checks installation preference and configures Content Tracker Reports to operate in secure mode.

     In secure mode, the same security criteria (role and account qualifications) that are used to limit Content Server search results for a particular user are also applied to the Content Tracker Report component's queries and the generated reports. Thus, it is possible that two different users running the Top Content Items report may see different results.

   - ❖ Leaving the checkbox blank (the default value) disables the security checks installation preference and configures Content Tracker Reports to operate in non-secure mode. This is the default setting.

     In non-secure mode, the additional role and account criteria used to restrict Content Server search results for a particular user are not applied to Content Tracker Report component's queries and the generated reports. Thus, it is possible for a user other than a system administrator to see information about content items that they would not be authorized to access and view.

Caution: If you have enabled Access Control Lists (ACLs) on your Content Server instance, the secure mode option in Content Tracker Reports does not work. For more information, see Access Control Lists and Content Tracker Reports Secure Mode (page 1-7).

Note: For more detailed information about the security checks installation preference and how it will affect the report queries and report results, refer to the *Content Tracker Administration Guide*.

7. Select the security checks installation preference checkbox or leave it blank.
8. Click **OK**.

   Component Wizard asks if you want to enable the Content Tracker Reports component.
9. Click **Yes**.

   The Content Tracker Reports component is listed as enabled on the Component List screen.
10. Exit the Component Wizard.
11. Restart Content Server to apply the updated installation parameters

    The Content Tracker Reports link is displayed in the Administration tray.

Restart Cycle for Master/Proxy Installations

When you are using a configurations that includes both Master and Proxy Content Servers, the web server filter plugin may require an extra restart. Otherwise, the Proxy Content Tracker may not be collecting data. Therefore, to ensure that the web server filter plugin for the Proxy instance is collecting data, perform the following restart sequence:

1. Install Content Tracker on the Master Content Server instance.
2. Restart the Master Content Server instance.
3. Restart the web server and the Master Content Server instance.

   The Master sctlog file starts.
4. Install Content Tracker on the Proxy Content Server instance.
5. Restart the Proxy Content Server instance.

6. Restart the web server and the Proxy Content Server instance.

   The Proxy sctlog file starts on the Master Content Server instance.

7. Restart the web server, the Proxy Content Server instance, and the Master Content Server instance.

   The Proxy sctlog file starts on the Proxy Content Server instance.

Note: For a general overview of support for Content Tracker in Master/Proxy configurations, see Master/Proxy Installations (page 1-8).

Chapter

3

POST-INSTALLATION

OVERVIEW

This section covers the following topics:

- ❖ Post-Installation Tasks and Considerations (page 3-1)
- ❖ Uninstalling Content Tracker (page 3-4)
- ❖ Re-Installing Content Tracker 10gR3 (page 3-8)
- ❖ Uninstalling Content Tracker Reports (page 3-8)
- ❖ Re-Installing Content Tracker Reports 10gR3 (page 3-12)

POST-INSTALLATION TASKS AND CONSIDERATIONS

This section covers the following topics:

- ❖ Grant Execution Permission to the Web Server Filter (HP-UX Only) (page 3-2)
- ❖ Grant Execution Permission to the Web Server Filter (HP-UX Only) (page 3-2)
- ❖ Custom Directory for Reduction Log Output (page 3-2)
- ❖ Post-Reduction Executable Set Up (page 3-3)
- ❖ Permissions for Data Directory Access (UNIX Only) (page 3-4)

Grant Execution Permission to the Web Server Filter (HP-UX Only)

If you have installed Content Tracker on an HP-UX operating system, Content Tracker will not automatically collect data in the data/ directory. To ensure proper data collection, you must manually give execution permission to the HP-UX web server filter as follows:

1. Open the following directory:

   <*install_dir*>/shared/os/hpux/lib/

2. Grant execution permission to the sctfp.sl file (the HP-UX web server filter). For example, a UNIX command would be:

   ```
   chmod 775 sctfp.sl
   ```

3. Restart the web server and Content Server.

Custom Directory for Reduction Log Output

During the installation process, Content Tracker automatically creates the directory that is used to store reduction log files. The default directory and path is:

<*install_dir*>/<*instance*>/custom/ContentTracker/log/

You can, however, create and use a custom directory for reduction log output files:

1. Create the new directory.
2. In a text editor, open the **sct.cfg** file:

   <*install_dir*>/<*instance*>/custom/ContentTracker/resources/sct.cfg

3. Locate the **SctReductionLogDir** configuration setting.
4. Delete the default **log** directory name and enter the custom directory name.
5. Save and close the **sct.cfg** file.
6. Restart the Content Server.

Post-Reduction Executable Set Up

Content Tracker provides support for running a user-supplied executable at the very end of data reduction.

Note: In the current version of Content Tracker, Windows.bat files are **not** executables and, therefore, will not execute. UNIX shell scripts are executables but only if the EXE bit is set in the file properties.

The following are required:

- ❖ The executable should reside in the following directory:

  <*install_dir*>/custom/ContentTracker/bin/

  There are no restrictions on its name.

- ❖ The executable should accept (or optionally ignore) three arguments:
  - logdate - in the form YYYYMMDD, which is the date (in local time) on which the data was originally collected.
  - logdir - full path of the directory that contains Content Tracker's output files.

Note: Content Tracker 7.5 and later no longer use an output/ directory for output data.

  - processedAll - true or false to indicate whether the population of the SctAccessLog output file ran to completion. A value of false indicates that generation of SctAccessLog was aborted, typically because of a timeout.

- ❖ The name of the executable should be listed as the value of the SctPostReductionExec configuration variable in Content Tracker' sct.cfg file located in the following directory:

  <*install_dir*>/custom/ContentTracker/resources/sct.cfg

  If you specified the name of the post-reduction executable when you installed Content Tracker, the name will be listed as the value for SctPostReductionExec. In this case, if you want to modify this value, you can do so using the Component Manager's configuration update function.

  However, if you did not specify a post-reduction executable during installation, then the name will not be listed in the sct.cfg file. In this case, you must manually edit the sct.cfg file and add the correct value to the SctPostReductionExec configuration variable.

If no value is specified or the property is not present, reduction proceeds without running an executable.

Important: If an executable is specified, data reduction is not considered to be complete until the executable has completed.

Important: If Stop Reduction is selected from the Content Tracker Data Engine Control Center and the user-specified executable is running, the executable process is stopped.

Important: When Stop Reduction is selected from the Content Tracker Data Engine Control Center, the reduction log contains the message “Reduction stopping at administrator's request.”

Permissions for Data Directory Access (UNIX Only)

To ensure that data collection is completed properly and ensure that files are written in the Content Tracker/data folder, the UNIX user running the web server must have Read, Write, and Delete permissions to the Content Tracker/data directory. The files created there are owned by the user. Additionally, the Content Server user viewing the log files also needs to have permission to access the Content Tracker /data directory.

To ensure proper permissions are set for UNIX users running the web server:

1. Add permission for the UNIX user running the web server to have Read, Write, and Delete permissions to the following directory:

   <*install_dir*>/custom/ContentTracker/data

2. Give the Content Server user permission to access the following directory:

   <*install_dir*>/custom/ContentTracker/data

UNINSTALLING CONTENT TRACKER

This section includes step-by-step instructions for uninstalling Content Tracker, and post-uninstall tasks and considerations. It covers the following topics:

❖ Uninstalling Content Tracker (page 3-5)

❖ Post-Uninstall Tasks and Considerations (page 3-7)

Caution: If you provided an optional executable to run after data reduction is completed, the uninstall will remove this file along with the <*install_dir*>/<*instance*>/custom/ContentTracker/bin/ directory. To preserve this executable, save it to a directory outside the Content Server hierarchy before performing the uninstall.

Uninstalling Content Tracker

You can uninstall the Content Tracker Reports component using either of the following methods:

- Uninstalling the Content Tracker Component using Component Manager (page 3-5)
- Uninstalling the Content Tracker Component using Component Wizard (page 3-6)

Uninstalling the Content Tracker Component using Component Manager

To uninstall the Content Tracker component using Component Manager:

1. Log in to Content Server as an administrator.
2. Select **Admin Server** from the Administration menu.

   The Content Admin Server page is displayed.
3. Click the name of the Content Server instance where the component will be uninstalled.

   The Content Admin Server <*instance_name*> page is displayed.
4. Click **Component Manager**.

   The Component Manager page is displayed.
5. Select the Content Tracker component in the Enabled Components list.
6. Click **Disable**.
7. Click **Start/Stop Content Server**.

   The Content Admin Server <*instance_name*> page is displayed.
8. Click **Restart**.

9. Click **Component Manager**.

   The Component Manager page is displayed and the Content Tracker component is in the Disabled Components list.

10. Select the Content Tracker component in the Uninstall Component drop-down menu.

11. Click **Uninstall**.

    Component Manager asks if you want to uninstall the component.

12. Click **OK**.

    Component Manager displays a message that the Content Tracker component was uninstalled successfully.

13. Select the link to return to the Component Manager.

    The Component Manager page is displayed.

14. Click **Start/Stop Content Server**.

    The Content Admin Server <*instance_name*> page is displayed.

15. Restart Content Server to apply the changes.

    The Content Tracker icon is removed from the Administration page.

Note: It is possible that after restarting Content Server, the Content Tracker icon is still visible. In this case, if you refresh your browser (clicking F5), the icon will be removed.

16. Restart the web server.

    The Content Tracker filter plugin is removed.

17. Restart Content Server.

    Content Tracker is completely removed from the instance.

Uninstalling the Content Tracker Component using Component Wizard

To uninstall the Content Tracker component using Component Wizard:

1. Start the Component Wizard by selecting **Start—All Programs—Content Server—<*instance*>—Utilities—Component Wizard** (Windows) or by running the *ComponentWizard* script in the */bin* directory (UNIX).

   The Component Wizard main screen and the Component List screen are displayed.

2. On the Component List screen, select the Content Tracker component and click **Disable**.
3. Restart Content Server.
4. On the Component List screen, select the Content Tracker component and click **Uninstall**.

   Component Wizard asks if you want to uninstall the Content Tracker component.
5. Click **Yes**.

   The Uninstall screen is displayed and lists the zip file contents that will be uninstalled.
6. Click **OK**.

   The Content Tracker component is removed from the Component List screen.
7. Exit the Component Wizard.
8. Restart Content Server to apply the changes.

   The Content Tracker icon is removed from the Administration page.

Note: It is possible that after restarting Content Server, the Content Tracker icon is still visible. In this case, if you refresh your browser (clicking F5), the icon will be removed.

9. Restart the web server.

   The Content Tracker filter plugin is removed.
10. Restart Content Server.

    Content Tracker is completely removed from the instance.

Post-Uninstall Tasks and Considerations

The following directories are not deleted when uninstalling Content Tracker 7.0 or earlier:

❖ *<install_dir>*/*<instance>*/custom/ContentTracker/data/

   This directory contains input data that Content Tracker has collected during Content Server sessions.

❖ *<install_dir>*/*<instance>*/custom/ContentTracker/log/
   This directory contains data reduction results log files that were generated when input data files were reduced.

❖ ***[Only for** Content Tracker **version 7.0 or earlier]***
   <install_dir>/*<instance>*/custom/ContentTracker/output/

This directory contains enhanced web log data file sets produced by Content Tracker as a result of the data reduction operation.

After uninstalling Content Tracker, these directories remain in the Content Server hierarchy to ensure that historical data is available when a new or update installation of Content Tracker is completed.

In addition to the above directories, the following files are not deleted:

- <*install_dir*>/<*instance*>/data/components/ContentTracker/config.cfg

  Contains the parameters that can be reconfigured after installation.

- <*install_dir*>/<*instance*>/data/components/ContentTracker/install.cfg

  Contains the preference data definitions and prompt answers.

- <*install_dir*>/<*instance*>/data/components/ContentTracker/<*backup Zip file*>

  This is a backup file that is created if the component is already installed and is being reinstalled.

RE-INSTALLING CONTENT TRACKER 10GR3

When you uninstall Content Tracker, the installation parameters are preserved and they become the preference values that are used in subsequent installations. These values will automatically populate the preference fields during the reinstallation—you do not need to re-enter the values. However, if you want to use the original Content Tracker default installation parameters, you will need to manually remove the previously installed preference values.

To re-install Content Tracker 10gR3 using default installation preference values:

1. Open the <*install_dir*>/data/components/ContentTracker/ directory.
2. Delete the install.cfg file.
3. Continue the installation procedure as documented in Instructions for Content Tracker New Install (page 2-5).

UNINSTALLING CONTENT TRACKER REPORTS

You can uninstall the Content Tracker Reports component using either of the following methods:

- ❖ Uninstalling the Content Tracker Reports Component using Component Manager (page 3-9)
- ❖ Uninstalling the Content Tracker Reports Component using Component Wizard (page 3-11)

Uninstalling the Content Tracker Reports Component using Component Manager

To uninstall the Content Tracker Reports component using Component Manager:

1. Log in to Content Server as an administrator.
2. Select **Admin Server** from the Administration menu.

   The Content Admin Server page is displayed.
3. Click the name of the Content Server instance where the component will be uninstalled.

   The Content Admin Server <*instance_name*> page is displayed.
4. Click **Component Manager**.

   The Component Manager page is displayed.
5. Select the Content Tracker Reports component in the Enabled Components list.
6. Click **Disable**.
7. Click **Start/Stop Content Server**.

   The Content Admin Server <*instance_name*> page is displayed.
8. Click **Restart**.
9. Click **Component Manager**.

   The Component Manager page is displayed and the Content Tracker Reports component is in the Disabled Components list.
10. Select the Content Tracker Reports component in the Uninstall Component drop-down menu.
11. Click **Uninstall**.

    Component Manager asks if you want to uninstall the component.
12. Click **OK**.

    Component Manager displays a message that the Content Tracker Reports component was uninstalled successfully.

13. Select the link to return to the Component Manager.

    The Component Manager page is displayed.

14. Click **Start/Stop Content Server**.

    The Content Admin Server <*instance_name*> page is displayed.

15. Restart Content Server to apply the changes.

    The Content Tracker Reports link is removed from the Administration tray.

Note: It is possible that after restarting Content Server, the Content Tracker Reports link is still visible. In this case, if you refresh your browser (clicking F5), the link will be removed.

Uninstalling the Content Tracker Reports Component using Component Wizard

To uninstall the Content Tracker Reports component using Component Wizard:

1. Start the Component Wizard by selecting **Start—All Programs—Content Server—<*instance*>—Utilities—Component Wizard** (Windows) or by running the *ComponentWizard* script in the /*bin* directory (UNIX).

   The Component Wizard main screen and the Component List screen are displayed.

2. On the Component List screen, select the Content Tracker Reports component and click **Disable**.
3. Restart Content Server.
4. On the Component List screen, select the Content Tracker Reports component and click **Uninstall**.

   Component Wizard asks if you want to uninstall the Content Tracker Reports component.

5. Click **Yes**.

   The Uninstall screen is displayed and lists the zip file contents that will be uninstalled.

6. Click **OK**.

   The Content Tracker Reports component is removed from the Component List screen.

7. Exit the Component Wizard.
8. Restart Content Server to apply the changes.

   The Content Tracker Reports link is removed from the Administration tray.

Note: It is possible that after restarting Content Server, the Content Tracker Reports link is still visible. In this case, if you refresh your browser (clicking F5), the link will be removed.

Re-Installing Content Tracker Reports 10gR3

When you uninstall Content Tracker Reports, the installation parameter is preserved and it becomes the preference value that is used in subsequent installations. This value will automatically populate the preference field during the reinstallation—you do not need to re-enter the value. However, if you want to use the original Content Tracker Reports default installation parameter, you will need to manually remove the previously installed preference value.

To re-install Content Tracker Reports 10gR3 using the default installation preference value:

1. Open the <*install_dir*>/data/components/ContentTracker Reports/ directory.
2. Delete the install.cfg file.
3. Continue the installation procedure as documented in Instructions for Content Tracker Reports New Install (page 2-13).

Chapter 4

Alternate Database Provider

Overview

This chapter covers the following topics:

About the Alternate Database Provider

Note: The following Content Server tables are required to ensure that Content Tracker Reports functions properly:

- Revisions
- Documents
- UserSecurityAttributes
- Users

Important: The architectural structure of Content Tracker v10gR3 has been modified and many of the files and database tables used in previous versions are no longer compatible with the current version. Although support for defining an alternate database provider has been retained, customers are responsible for replicating relevant Content Server tables before performing any queries against the Content Tracker output.

Important: Content Tracker does not work with IBM DB2 as an alternate database provider. Therefore, the default SystemDatabase provider must be used.

Setting up an alternate database and defining the corresponding alternate database provider offers two operational advantages and can help optimize tracking operations by:

- Detaching the reduced data output tables from the Content Server database.

  After an alternate database provider is defined and operational, Content Tracker automatically stores all reduced data in the alternate database using the custom provider information. As a result, Content Tracker automatically creates the Content Tracker tables in the alternate database and these tables are never created in the Content Server database.

- Preventing the Content Tracker database activity from potentially affecting Content Server operations.

  Because the Content Tracker tables are not included in the Content Server database, the Content Tracker database activity will not interfere with Content Server processing.

Defining the Alternate Provider after Content Tracker Installation

Important: Setting up an alternate database provider is optional and there is no support for this as part of the Content Tracker component.

1. Access the Providers page in the Content Server instance and create a **database provider** named SCT_Database using appropriate connection information.

   For more detailed information about creating database providers, refer to the Understanding Providers topic included in the Setting Security section of the *Content Server System Administration Guid*e.

2. After the database provider is created and operational, open the **provider.hda** file in a text editor:

   <*install_dir*>/<*instance*>/data/providers/sct_database/provider.hda

3. Add the following lines:

   ```
   ProviderConfig=intradoc.server.DbProviderConfig

   QueryResourceFile=../custom/ContentTrackerReports/resources/contentt
   rackerreports_query.htm

   QueryResourceTables=ContentTrackerReports_Queries
   ```

4. Save and close the **provider.hda** file.
5. If necessary, restart the Content Server.

DEFINING THE ALTERNATE PROVIDER BEFORE CONTENT TRACKER INSTALLATION

Use the following procedure to create the alternate database provider before Content Tracker is installed:

1. Access the Providers page in the Content Server instance and create a **database provider** named SCT_Database using appropriate connection information.

   For more detailed information about creating database providers, refer to the Understanding Providers topic included in the Setting Security section of the *Content Server System Administration Guid*e.

2. Install Content Tracker and Content Tracker Reports.
3. Open the **provider.hda** file in a text editor:

   <*install_dir*>/<*instance*>/data/providers/sct_database/provider.hda

4. Add the following lines:

   ```
   ProviderConfig=intradoc.server.DbProviderConfig

   QueryResourceFile=../custom/ContentTrackerReports/resources/contentt
   rackerreports_query.htm

   QueryResourceTables=ContentTrackerReports_Queries
   ```

5. Save and close the **provider.hda** file.
6. Restart the Content Server.

Appendix

A

CONTENT TRACKER SUPPORT FOR CONTENT SERVER CONFIGURATIONS

OVERVIEW

This appendix covers the following topics:

Concepts

Tasks

CONTENT TRACKER 10GR3 CONFIGURATION SETTINGS

The following table lists the default values of the configuration settings used in the current version of Content Tracker. These configuration variables are contained in the Content Tracker configuration file:

<install_dir>/custom/ContentTracker/resources/sct.cfg

Note: Component Manager preferences and Update fields introduced in Content Tracker version 10.1.3.3.3 include some configuration settings that automatically override certain sct.cfg settings. The preferences are described in Installing Content Tracker (page 2-5) and include the following: SctDoNotArchive (overrides the sct.cfg setting SctMaxRecentCount), SctDoNotPopulateAccessLogColumns, SctMaxRecentCount (overrides the sct.cfg setting with the same name), SctSimplifyUserAgent, and SctTrackContentAccessOnly.

Config. Setting	Default Value	Remarks
SctAutoTruncateDataStrings	FALSE	Used by: JAVA Determines whether the reduction process will truncate data strings to fit into the corresponding table column.
SctComponentDir	*<install_dir>*/custom/ContentTracker/	Used by: JAVA Path to the directory where Content Tracker is installed.
SctDebugLogEnabled	FALSE	Used by: JAVA Set TRUE to enable Java code execution trace. Used with SctDebugLogFilePath.
SctDebugLogFilePath	*<install_dir>*/custom/ContentTracker/log/SCT_DEBUG_TRACE.log	Used by: JAVA Directory for Java code execution trace. Used with SctDebugLogEnabled.
SctDebugServiceBinderDumpEnabled	FALSE	Used by: JAVA Set TRUE to enable diagnostic output of Service DataBinder objects during Service logging.

Config. Setting	Default Value	Remarks
SctExternalUserLogEnabled	TRUE	Used by: JAVA Set TRUE to enable replication of External user account and role information to UserSecurityAttributes table.
SctFilterPluginLogDir	<*install_dir*>/custom/ContentTracker/data/	Used by: filter plugin Path to the directory where filter plugin will store the event logs.
SctIdcAuthExtraConfigParams	SctFilterPluginLogDir, SctLogEnabled, SctIgnoreFileTypes, SctLogSecurity, SctUseLock, SctLockPort	List of Content Tracker configuration parameters that are passed along to the filter plugin, merged programmatically into idcAuthExtraConfigParams by Sct startup filter
SctIgnoreDirectories	/stellent/resources/;/stellent/common/	Used by: filter plugin Directs filter plugin to disregard URLs contained within the listed directory roots.
SctIgnoreFileTypes	gif,jpg,js,css	Used by: filter plugin Directs filter plugin to disregard URLs with the listed filetypes.
SctLockPort	4477	Used by: filter plugin Network port used by filter plugin to connect to Content Server Lock Provider.
SctLogDir	<*install_dir*>/custom/ContentTracker/data/	Used by: JAVA Path to the directory(s) where Content Tracker looks for the raw event logs - sctLog, etc. May be multi-valued, e.g. dir1;dir2;…;dir*n*.

Config. Setting	Default Value	Remarks
SctLogEnabled	TRUE	Used by: filter plugin, JAVA If False, directs service handler filters and web server filter plugin to ignore all events and create no logs. This is the Content Tracker Master On/Off switch.
SctLogSecurity	TRUE	Used by: filter plugin, JAVA If true, directs filter plugin to record IMMEDIATE_RESPONSE_PAGE events in the sctSecurityLog event log, and the reduction process to read the event log.
SctMaxRecentCount	5	Used by: JAVA Maximum number of days worth of reduced data kept in the “Recent” state. Overflow from Recent is moved to Archive state. If Content Tracker version 10.1.3.3.3 is installed, then the default is automatically set to 60.
SctMaxRereadTime	3600	Used by: JAVA Maximum number of seconds that can occur between consecutive references by a particular user to a particular content item, e.g. a PDF file, and have the adjacent references be considered a single sustained access. Consecutive references which occur further apart in time count as separate accesses.
SctPostReduction Exec	[none]	Used by: JAVA Path to Post Reduction Executable (assumed to be in <cs_root>/custom/ContentTracker/bin/)
SctProxyNameMax Length	50	Used by: JAVA Maximum number of characters in the name of any Content Server proxy server in the configuration. Used to increase the size of user name fields in Content Tracker table creation.

Config. Setting	Default Value	Remarks
SctReductionAvailableDatesLookback	0	Used by: JAVA Used with SctReductionRequireEventLogs to limit Available Dates range. Unit = Days. Zero = unlimited.
SctReductionLogDir	<*install_dir*>/custom/ContentTracker/log/	Used by: JAVA Path to the directory where the Content Tracker reduction logs are stored.
SctReductionRequireEventLogs	TRUE	Used by: JAVA Used in Detached configurations. FALSE means proceed with Reduction even if no event logs are found.
SctScheduledReductionEnable	TRUE	Used by: JAVA Used in Multi-JVM configurations to select which Content Server instance performs the reduction.
SctSnapshotEnable	FALSE	Used by: JAVA Set TRUE to enable Snapshot functions. Set from Data Engine Control Center.
SctSnapshotLastAccessEnable	FALSE	Used by: JAVA Set TRUE to enable Last Access Date Snapshot function. Set from Data Engine Control Center.
SctSnapshotLastAccessField	[none]	Used by: JAVA Metadata field name for Last Access Date, e.g. xLastAccessDate. Set from Data Engine Control Center.
SctSnapshotLongCountEnable	FALSE	Used by: JAVA Set TRUE to enable "Long" interval access count Snapshot function. Set from Data Engine Control Center.
SctSnapshotLongCountField	[none]	Used by: JAVA Metadata field name for Long Interval Count, e.g. xAccessesInLast90Days. Set from Data Engine Control Center.

Config. Setting	Default Value	Remarks
SctSnapshotLong CountInterval	[none]	Used by: JAVA Number of days for “Long” Interval. Set from Data Engine Control Center.
SctSnapshotShort CountEnable	FALSE	Used by: JAVA Set TRUE to enable “Short” interval access count Snapshot function. Set from Data Engine Control Center.
SctSnapshotShort CountField	[none]	Used by: JAVA Metadata field name for Short Interval Count, e.g. xAccessesInLast10Days. Set from Data Engine Control Center.
SctSnapshotShort CountInterval	[none]	Used by: JAVA Number of days for “Short” Interval. Set from Data Engine Control Center.
SctTrackerInfoFile	<*install_dir*>/custom/ContentTracker/bin/trackerinfo.txt	Used by: JAVA Path to special configuration file used to maintain Content Tracker Scheduler parameters.
SctUrlMaxLength	3000	Used by: JAVA Maximum expected length (characters) for URL fields. Used to determine column widths when creating tables. There may be several such columns in a given table.
SctUseGMT	FALSE	Used by: filter plugin, JAVA Set TRUE for logged event times to be converted to Universal Coordinated Time. FALSE uses local time.
SctUseLock	TRUE	Used by: filter plugin If true, directs filter plugin to obtain lock from Content Server Lock Provider before writing to raw log files (sctLog-yyyymmdd.txt, etc.). Otherwise, no locks enforced and sequence numbers assigned internally.

Setting Content Tracker Configuration Variables

To set or edit any of the Content Tracker configuration variables:

1. In a text editor, open the sct.cfg file:

   <*install_dir*>/custom/ContentTracker/resources/sct.cfg
2. Locate the configuration variable to be edited.
3. Enter the applicable value.
4. Save and close the sct.cfg file.
5. Restart Content Server to apply the changes.

SUPPORTED CONTENT SERVER CONFIGURATIONS

Gathering information about content accesses has shifted from the web server to Content Server, which makes Content Tracker independent of web server type. This eliminates the need for Content Tracker to depend on the web server to write an event log in a particular format. As a result of eliminating web server dependencies, Content Tracker now supports installations with multiple web servers and installations in which the web server(s) does not have direct access to the Content Server storage volume. For the current release of Content Tracker, any given Content Server instance belongs to one of three configuration classes:

- Standard installation (page A-7)
- Cluster installation (page A-8)
- Detached installation (page A-8)

Standard installation

This configuration has a single file system shared between web server(s) and the Content Server instance. It can have more than one web server, but only one Content Server “execution context” (i.e. JVM - see the Cluster configuration below for comparison. This includes almost all simple installations. Refer to Configuring Content Tracker for a Standard Installation (page A-8).

Cluster installation

This configuration has a single file system shared between web server(s) and multiple Content Server execution contexts running on separate JVMs, all sharing a single instance directory tree. It can have multiple web servers, possibly working through a load balancer. This installation requires manual configuration. Refer to Configuring Content Tracker for Cluster Installations (page A-8).

Detached installation

This configuration does not allow content access via the web server. Sct event log files are not used. All content access is done via an application server such as BEA, IBM, or a custom front end. This installation requires manual configuration. Refer to Configuring Content Tracker for a Detached Installation (page A-16).

Configuring Content Tracker for a Standard Installation

Content Tracker does not require manual changes in the standard Content Server installation. Web server filter plugins write event log files (all sctLog files) with a hostname|port number suffix in the filename. This aids in matching events in the different log types. Content Tracker does a wildcard lookup for event logs, so it will find the logs from all the web servers. For a brief definition of a standard Content Server installation, refer to Standard installation (page A-7).

Configuring Content Tracker for Cluster Installations

This section provides two examples to configure Content Tracker for cluster installations:

- Example 1: Configuring Content Tracker for a Cluster Installation (Generic Instructions) (page A-8)
- Example 2: Configuring Content Tracker for a Cluster Installation (UNIX Instructions) (page A-12)

Example 1: Configuring Content Tracker for a Cluster Installation (Generic Instructions)

You need to move specific fields from sct.cfg to intradoc.cfg so that the execution contexts, each of which is assumed to have its own intradoc.cfg, can have different

Content Tracker configuration values. For a brief definition of a clustered Content Server installation, refer to Cluster installation (page A-8).

Scheduled Reductions

For scheduled reductions, you need to ensure that only one context performs the reduction as follows:

1. Select a context (JVM) that will perform the scheduled reductions.
2. In a text editor, open the sct.cfg and intradoc.cfg files:

   <*install_dir*>/custom/ContentTracker/resources/sct.cfg

   <*cluster_stub_dir*>/bin/intradoc.cfg

Note: Stub directories are created in cluster configurations that use two or more Content Server instances that execute on different machines with separate JVMs but share a single directory tree and database. In this configuration, the use of different JVMs creates problems involving the Content Tracker event logs and scheduled reductions. For more detailed information about cluster stub directories, refer to the *Content Server Cluster Configuration Guide for Windows* or the *Content Server Cluster Configuration Guide for UNIX*.

3. Move the SctScheduledReductionEnable configuration variable from the sct.cfg file to the intradoc.cfg file for all contexts.
4. Set SctScheduledReductionEnable to “true” for the context that will perform the scheduled reductions and set the value to “false” for all other contexts.
5. Save the changes to the sct.cfg and intradoc.cfg files.

Event Logs

There is a special issue for configurations in which web servers are 'connected' or 'bridged' across more than one execution context (JVM). This will typically happen if a load balancer is employed between the web servers and the Content Server execution contexts. The Content Tracker web server filter plugin uses a lock provider to ensure that different threads don't conflict with each other while writing the Content Tracker event logs.

However, this may not work for clusters with bridged web server(s) because normal Java Object locks don't work across JVMs. The workaround for this situation involves segregating the output for each of the contexts into a separate directory. The reduction engine then gathers up all the files. To segregate the data output for each context:

1. In a text editor, open the sct.cfg and intradoc.cfg files:

   <*install_dir*>/custom/ContentTracker/resources/sct.cfg
   <*cluster_stub_dir*>/bin/intradoc.cfg

2. Move the SctFilterPluginLogDir configuration variable from the sct.cfg file to the intradoc.cfg file for all contexts.

3. Create a /data/ directory for each context (in each node in the cluster configuration). For example:

   In nodeOne, the following directory is created:

   ```
   <cluster_stub_dir>/custom/ContentTracker/data1/
   ```

   In nodeTwo, the following directory is created:

   ```
   <install_dir>/custom/ContentTracker/data2/
   ```

   ... etc.

Note: The /data/ directory that is created in each node in a cluster configuration should be accessible by file server (that is, the server where Content Server is installed) and have all the permissions (read, write, delete).

4. In the intradoc.cfg file, set the SctFilterPluginLogDir configuration variable for each context (in each node in the cluster configuration) to the corresponding data directory path. For example:

   In nodeOne, the SctFilterPluginLogDir configuration variable is set as follows:

   ```
   SctFilterPluginLogDir=c:/stellent/idcm1/custom/
   ContentTracker/data1/
   ```

   In nodeTwo, the SctFilterPluginLogDir configuration variable is set as follows:

   ```
   SctFilterPluginLogDir=c:/stellent/idcm1/custom/
   ContentTracker/data2/
   ```

   ... etc.

5. Save the changes to the sct.cfg and intradoc.cfg files.

Reduction

The reduction engine needs to know where to look for all the different context event log files. To ensure that each Content Tracker event log is found:

1. In a text editor, open the sct.cfg file:

   <*install_dir*>/custom/ContentTracker/resources/sct.cfg

2. Expand the SctLogDir configuration variable value to include all the context data directories (created in the Event Logs sub-section above). Include them in a semi-colon delimited path. For example:

```
SctLogDir = c:/stellent/idcm1/custom/ContentTracker/data/;
<cluster_stub_dir>/custom/ContentTracker/data1/;<cluster_stub_dir>/
custom/ContentTracker/data2/
```

Note: The first directory in SctLogDir configuration variable will also be used as a root for the recent and archive directories. This will normally be c:/stellent/idcm1/custom/ContentTracker/data/.

3. Save the changes to the sct.cfg file.

Data Collection

To ensure that Content Tracker works in the cluster installation, the following procedure must be completed on each node in the cluster:

1. Open the following Content Server directory:

   <*install_dir*>/data/users/

2. Copy the SystemFilters.hda file.
3. Paste the copied SystemFilters.hda file into the following Content Server directory:

   <*cluster_stub_dir*>/data/users/

   where <*cluster_stub_dir*> is the applicable directory for this node (for example, <*cluster_stub1_dir*> for nodeOne, <*cluster_stub2_dir*> for nodeTwo, etc.).

4. Open the following Content Server directory:

   <*install_dir*>/shared/os/<*os_name*>/lib/

   where <*os_name*> is the name of your operating system (win32, linux, solaris, aix, or hpux).

5. Copy the applicable Content Tracker web server filter file.

Note: The Content Tracker web server filter name uses the following format:

sctfp.<*extension*>

For Windows, the web server filter is named sctfp.dll. For Solaris, AIX, and Linux the web server filter is named sctfp.so. For HP-UX, the web server filter is named sctfp.sl.

6. Paste the copied web server filter file into the following Content Server directory:

   <*cluster_stub_dir*>/shared/os/<*os_name*>/lib/

where <*cluster_stub_dir*> is the applicable directory for this node (for example, <*cluster_stub1_dir*> for nodeOne, <*cluster_stub2_dir*> for nodeTwo, etc.), and where <*os_name*> is the name of your operating system (win32, linux, solaris, aix, or hpux).

7. Restart the web server and Content Server.

Example 2: Configuring Content Tracker for a Cluster Installation (UNIX Instructions)

The step-by-step example in this section demonstrates how to set up Content Tracker in a cluster configuration. This particular cluster configuration uses an NFS file sharing system, on an IBM HTTP Server (IHS/Apache) with an AIX operating system.

Note: The information provided in this section should be used in addition to the information provided in the *Content Server Cluster Configuration Guide for Windows* or the *Content Server Cluster Configuration Guide for UNIX.*

To support a cluster installation, some manual configurations are required:

1. Install and enable the Content Tracker component using either the Component Manager or the Component Wizard—see Instructions for Content Tracker New Install (page 2-5).

2. In a text editor, open Content Server's intradoc.cfg file on the cluster's first node (node1):

   Configurations using network attached storage (NAS):

   <*scs_stub*>/bin/intradoc.cfg

   Configurations using storage area networks (SAN):

   <*scs_shared*>/bin/intradoc.cfg

3. Add the following configuration variables and values:

   Configurations using network attached storage (NAS):

   ```
   SctScheduledReductionEnable=true

   SctFilterPluginLogDir=<scs_stub>/custom/ContentTracker/
   data1/

   SctSchedulerLogDir=<scs_stub>/custom/ContentTracker/log1/
   ```

   Configurations using storage area networks (SAN):

   ```
   SctScheduledReductionEnable=true
   ```

```
SctFilterPluginLogDir=<scs_shared>/custom/ContentTracker/
data1/
```

```
SctSchedulerLogDir=<scs_shared>/custom/ContentTracker/log1/
```

4. In a text editor, open Content Server's intradoc.cfg file on the cluster's second node (node2):

   Configurations using network attached storage (NAS):

   <*scs_stub*>/bin/intradoc.cfg

   Configurations using storage area networks (SAN):

   <*scs_shared*>/bin/intradoc.cfg

5. Add the following configuration variables and values:

   Configurations using network attached storage (NAS):

   ```
   SctScheduledReductionEnable=false
   ```

   ```
   SctFilterPluginLogDir=<scs_stub>/custom/ContentTracker/
   data2/
   ```

   Configurations using storage area networks (SAN):

   ```
   SctScheduledReductionEnable=false
   ```

   ```
   SctFilterPluginLogDir=<scs_shared>/custom/ContentTracker/
   data2/
   ```

6. In a text editor, open Content Tracker's sct.cfg file on the cluster's first node (node1):

   <*scs_shared*>/custom/ContentTracker/resources/sct.cfg

7. Add the following configuration variables and values:

   ```
   SctScheduledReductionEnable=true
   ```

   ```
   SctFilterPluginLogDir=<scs_shared>/custom/ContentTracker/data/
   ```

   ```
   SctSchedulerLogDir=<scs_shared>/custom/ContentTracker/log/
   ```

8. Expand the SctLogDir configuration variable value to include all the context data directories. Include them in a semi-colon delimited path as follows:

   SctLogDir=<*scs_shared*>/custom/ContentTracker/data/;<*scs_shared*>/custom/ContentTracker/data1/;<*scs_shared*>/custom/ContentTracker/data2/

9. On the first node (node1), open a command prompt and create Content Tracker data collection folders from the <*scs_stub*> directory as follows:

   a. `mkdir custom`

   b. `mkdir custom/ContentTracker`

   c. `mkdir custom/ContentTracker/data1`

   d. `mkdir custom/ContentTracker/log1`

10. On the first node (node1), create a Content Tracker data collection “cron destination” folder from the <*scs_shared*>/custom/ContentTracker directory as follows:

    a. `mkdir data1`

11. On the second node (node2), open a command prompt and create Content Tracker data collection folders from the <*scs_stub*> directory as follows:

    a. `mkdir custom`

    b. `mkdir custom/ContentTracker`

    c. `mkdir custom/ContentTracker/data2`

    d. `mkdir custom/ContentTracker/log2`

12. On the second node (node2), create a Content Tracker data collection “cron destination” folder from the <*scs_shared*>/custom/ContentTracker directory as follows:

    a. `mkdir data2`

13. In a text editor, open the Content Server’s SystemFilters.hda file on the cluster’s first node (node1):

    <*scs_stub*>/data/users/SystemFilters.hda

14. Add two Content Tracker filter lines (sctfpPlugin and sctfp) so the modified file matches at least the last two lines above the @end as follows:

```
===========================
@Properties LocalData
@end
@ResultSet IdcAuthPlugins
2
iapExportedSymbolName
iapFileNameRoot
sctfpPlugin
sctfp
@end
===========================
```

15. In a text editor, open the Content Server's SystemFilters.hda file on the cluster's second node (node2):

    <*scs_stub*>/data/users/SystemFilters.hda

16. Add two Content Tracker filter lines (sctfpPlugin and sctfp) so the modified file matches at least the last two lines above the @end as follows:

    ```
    ===========================
    @Properties LocalData
    @end
    @ResultSet IdcAuthPlugins
    2
    iapExportedSymbolName
    iapFileNameRoot
    sctfpPlugin
    sctfp
    @end
    ===========================
    ```

17. On the first node (node1), open a command prompt and copy the Content Tracker filter plug-in module from the share to the stub as follows:

    ```
    cp <scs_shared>/shared/os/aix/lib/sctfp.so <scs_stub>/shared/
    os/aix/lib
    ```

18. On the second node (node2), open a command prompt and copy the Content Tracker filter plug-in module from the share to the stub as follows:

    ```
    cp <scs_shared>/shared/os/aix/lib/sctfp.so <scs_stub>/shared/
    os/aix/lib
    ```

19. Restart node1 IHS via:

    /usr/HTTPServer/bin/apachectl restart

20. Restart node1 SCS via:

    <scs_stub>/etc/idcserver_ctrl restart

21. Restart node2 IHS via:

    /usr/HTTPServer/bin/apachectl restart

22. Restart node2 SCS via:

    <scs_stub>/etc/idcserver_ctrl restart

Important: If you are using a high availability file system, such as a fibre-attached storage area network (SAN), you do not need to perform steps 23 through 25.

23. Create a shell script for node1 that will later be scheduled via AIX cron daemon. The directory for this script should not reside within the Content Server folder structure. This prevents accidental removal during upgrades, component changes, etc. Refer to the following basic example:

    ```
    #!/bin/ksh

    mv <scs_stub>/custom/ContentTracker/data1/* <scs_shared>/
    custom/ContentTracker/data1
    ```

24. Create a shell script for node2 that will later be scheduled via AIX cron daemon. Refer to the following basic example:

    ```
    #!/bin/ksh

    mv <scs_stub>/custom/ContentTracker/data2/* <scs_shared>/
    custom/ContentTracker/data1
    ```

25. Add the scripts created in steps 23 and 24 to the AIX user's crontab for both node1 and node2. Set cron to run after 12:00 AM. For example, 12:30 AM is recommended. It should be set before the time listed in the node1 trackerinfo.txt file for "CTrackerTimeToRun":

    ```
    <scs_shared>/custom/ContentTracker/bin/trackerinfo.txt
    ```

Caution: DO NOT run manual reductions from the Content Tracker Reduction tab on the Data Engine Control Center. Manual reductions may result in a loss of data.

Configuring Content Tracker for a Detached Installation

To support a detached installation, some manual configuration changes are required. You need to configure the reduction engine to ensure that it does not look for the Content Tracker event log files. You also need to provide a limit to the GetAvailableDates logic which supplies the Admin user interface with a list of dates eligible for reduction. For a brief definition of a detached Content Server installation, refer to Detached installation (page A-8).

No Event Logs

To ensure that the reduction engine does not search for Content Tracker event log files:

1. In a text editor, open the sct.cfg file:

   <*install_dir*>/custom/ContentTracker/resources/sct.cfg

2. Set the following configuration variable:

   ```
   SctReductionRequireEventLogs=False
   ```

   This allows a scheduled reduction to proceed in the absence of the usual event logs. It also signals GetAvailableDates to look in the SctAccessLog table for Content Server operation dates, rather than looking for existing Content Tracker event log files as it normally does.

3. Save the changes to the sct.cfg file.

Date Limit

It is also necessary to limit how far back in time GetAvailableDates looks if SctReductionRequireEventLogs=False.

1. In a text editor, open the sct.cfg file:

   <*install_dir*>/custom/ContentTracker/resources/sct.cfg

2. Set the following configuration variable:

   ```
   SctReductionAvailableDatesLookback=n
   ```

   where:
   n is the maximum number of days in the past to consider. Content Tracker will look in the SctAccessLog table for date stamps within the n day limit and this list will be the basis for the AvailableDates list sent to the Admin applet GUI. If n=0, there is no limit (not advised, but allowed).

Note: The SctReductionAvailableDatesLookback configuration variable is only honored if SctReductionRequireEventLogs=False.

3. Save the changes to the sct.cfg file.

Appendix

B

UPDATE INSTALLATIONS

OVERVIEW

This appendix includes information relevant to updates from a previous release of Content Tracker.

Caution: Backwards compatibility is undefined. The instructions in this appendix are from previous versions of the documentation, and at the time of print, update installations have not been tested.

DATABASE ISSUES

Sybase Database Issues

Sybase issues noted in Sybase Database Issues (page 1-5) are likely relevant to upgrading from Content Tracker 6.2 or 6.5 to version 7.0, 7.5 or 10gR3.

RECOMMENDATIONS BEFORE UPGRADING TO CONTENT TRACKER 10GR3

Caution: Although every effort has been made to ensure data integrity and preservation during the database table upgrade process, unforeseeable circumstances in each system configuration might leave the database in an inconsistent state after the tables are upgraded. For this reason, users are strongly encouraged to employ reasonable precautions before beginning the upgrade installation of Content Tracker 10gR3.

❖ **Recommended Precautions:**

Content Tracker 7.0 (or earlier) users who want to save their data should plan to back up their database before attempting the upgrade installation. During the installation, Content Tracker 10gR3 will eliminate the following: SctEnhanced, SctCustom, SctDocInfo, SctDocMetaDefinition, SctDocTypes, SctAccounts and the Archive pair for each.

❖ **Possible Name Conflicts:**

Beginning with Content Tracker 7.5, the raw data files include the web server host name and port number (Sctlog-yyyymmdd-<webhostportnum>.txt). Although a new naming convention is used, Content Tracker may continue to locate old data sets that use the previous naming convention (sctLog-yyyymmdd.txt). This could cause problems during the reduction process. Users should ensure that all such files are removed from the relevant directories.

Compatibility of Existing SQL Reports: Content Tracker Reports 7.0 or Earlier

Content Tracker 7.5 and later employ major architectural revisions of both the Content Tracker and the Content Tracker Reports components. Because of the significant schema and design changes to the components, there is no feasible way to guarantee that SQL report queries used with 7.0 and earlier versions of Content Tracker and Content Tracker Reports are compatible with the 7.5 and later versions.

However, the following list details the changes that were made and the reasons for them. This information should ensure that most users will experience few problems in adapting their queries to accommodate the new architectural and schema changes.

- Access information gathering has shifted from the web server to Content Server which makes Content Tracker independent of web server type. This eliminates the need for Content Tracker to depend on the web server to write an event log in a particular format.
- As a result of eliminating web server dependencies, installing the Content Tracker and Content Tracker Reports components is greatly simplified. Furthermore, the number and type of supported server configurations has expanded considerably. For example, Content Tracker now supports installations with multiple web servers and installations in which the web server(s) does not have direct access to the Content Server storage volume.
- Content Tracker no longer logs content item metadata so the content metadata tables are no longer generated. The standard Content Server metadata tables are used for content item metadata. This reduces the processing that needs to occur. It also ensures that all metadata is accessible to Content Tracker and that metadata values are up-to-the-minute current and accurate. Additionally, eliminating redundant output tables also stops redundant content metadata logging.
- Content Tracker continues to log user metadata and the applicable Content Tracker metadata tables in the database are updated during the reduction process.This ensures historically accurate user metadata.
- Static URL references are collected and logged by the web server filter plugin and Content Server service calls are logged by the service handler filter. Both types of event details are recorded in a table (SctAccessLog) which replaces the SctEnhanced table. used in Content Tracker v7.0 and earlier.
- The structural changes in Content Tracker v7.5 and later have increased the scope and improved the granularity of managed content usage reporting. This is due to eliminating the use of web server log files, expanding the collection of both static URL accesses and Content Server service calls, and ensuring that Content Tracker has access to all metadata values (both user and content item).

  Instead of reporting on page/object accesses at the URL level, Content Tracker can now track activity at the template/fragment level. This enables users to see how the various content item elements are being used. This means that Content Tracker can perform more interesting analysis on Site Studio sites and other applications that don’t use the Content Server’s native interface.
- Search results can incorporate specific data about user accesses. Custom metadata fields are used to record user access activity. Tracking results included in reports can reflect the popularity of certain content items or provide access data during specific time periods. Access tracking can include both internal and external users.

❖ The security checks feature optionally enforces user role and account privilege verification. When enabled, the security checking function filters the data based on role/account permissions of the user requesting the report. Consequently, different users may see different results after generating the same report. Otherwise, default SQL report queries generate reports with identical data for all users without regard for their user/account memberships.

Caution: If you have enabled Access Control Lists (ACLs) on your Content Server instance, the secure mode option in Content Tracker Reports does not work. For more information, see Access Control Lists and Content Tracker Reports Secure Mode (page 1-7).

For more detailed information about particular files, tables, and directories, refer to the *Content Tracker Administration Guide*.

A Note About Content Server Updates

If you are planning to update both your Content Server software and your Content Tracker, perform the following steps in the order listed:

1. Save any files or directories that you feel are important such as the data/, output/, and log/ directories. Move the saved directories to the specified location in the content server hierarchy. See Instructions for Content Tracker Update Install (page B-4).
2. Uninstall Content Tracker. For older versions, use the Setup program from the applicable release—see Uninstalling Content Tracker (page 3-5). For newer versions, use either the Component Manager or Component Wizard—see Uninstalling Content Tracker (page 3-5).
3. Perform the Content Server update installation.
4. Install the new release of Content Tracker. See Installing Content Tracker (page 2-5).

Instructions for Content Tracker Update Install

Because of the extensive architectural and table schema changes in the current version of Content Tracker, the previous reduction data sets (corresponding data output files and tables) are no longer compatible with the 10gR3. For this reason, this section includes general instructions for updating Content Tracker from previous versions as follows:

- Updating to Content Tracker 10gR3 from Content Tracker 6.5 or Earlier (page B-5)
- Updating to Content Tracker 10gR3 from Content Tracker 7.0 (page B-5)
- Updating to Content Tracker 10gR3 from Content Tracker 7.5 (page B-6)

Updating to Content Tracker 10gR3 from Content Tracker 6.5 or Earlier

1. Save any of the reduced data sets (and raw data logs, if desired) from the Content Server database or other files, tables, and directories that contain data that you feel is important.
2. Uninstall Content Tracker. Use the Setup program from the older (currently installed) release. See Uninstalling Content Tracker (page 3-5). Remove the ContentTracker/ directory and all of its subdirectories:

   <*install_dir*>/custom/ContentTracker/

Caution: The names of the raw data files include the web server host name and port number. Although this new naming convention is used, the current version of Content Tracker may continue to locate old data sets that still exist. This could cause problems during the Content Tracker 10gR3 reduction process.

3. Install the new release of Content Tracker. See Installing Content Tracker (page 2-5).

Note: Content Tracker 10gR3 no longer logs content metadata. Therefore, installing the current version (10gR3) may delete some database tables created by previous versions of Content Tracker. The tables no longer created include SctCustom, SctDocInfo, SctDocMetaDefinition, SctDocTypes, and SctAccounts. Also, a new table, SctAccessLog, replaces the previous SctEnhanced table.

Updating to Content Tracker 10gR3 from Content Tracker 7.0

1. Save any of the reduced data sets (and raw data logs, if desired) from the Content Server database or other files, tables, and directories that contain data that you feel is important.
2. Uninstall Content Tracker. Use either the Component Manager or the Component Wizard. See Uninstalling Content Tracker (page 3-5).
3. Remove the ContentTracker/ directory and all of its subdirectories:

<install_dir>/custom/ContentTracker/

Caution: The names of the raw data files include the web server host name and port number. Although this new naming convention is used, the current version of Content Tracker may continue to locate old data sets that still exist. This could cause problems during the Content Tracker v10gR3 reduction process.

4. Install the new release of Content Tracker. Use either the Component Manager or the Component Wizard. See Installing Content Tracker (page 2-5).

Note: Content Tracker 10gR3 no longer logs content metadata. Therefore, installing the current version (10gR3) may delete some database tables created by previous versions of Content Tracker. The tables no longer created include SctCustom, SctDocInfo, SctDocMetaDefinition, SctDocTypes, and SctAccounts. Also, a new table, SctAccessLog, replaces the previous SctEnhanced table.

Updating to Content Tracker 10gR3 from Content Tracker 7.5

1. Save any of the reduced data sets (and raw data logs, if desired) from the Content Server database or other files, tables, and directories that contain data that you feel is important.

Note: This step is actually for precautionary purposes only. It is actually optional when you upgrade from Content Tracker 7.5 to Content Tracker 10gR3 because the data files and database table data are not eliminated during the Content Tracker 7.5 uninstall procedure.

2. Uninstall Content Tracker. Use either the Component Manager or the Component Wizard. See Uninstalling Content Tracker (page 3-5).
3. Install the new release of Content Tracker. Use either the Component Manager or the Component Wizard. See Instructions for Content Tracker New Install (page 2-5).

Instructions for Content Tracker Reports Update Install

To update the Content Tracker Reports component:

1. Click the **Admin Server** applet icon on the Administration page.

   The Content Admin Server page is displayed.
2. Click the applicable Content Server instance button.
3. Click the **Component Manager** link.

The Component Manager page is displayed.

4. Select **Content Tracker Reports** from the Enabled Components box.
5. Click **Disable**.

   Content Tracker is moved to the Disabled Components box and is disabled.

6. Install the new release of Content Tracker Reports into the same Content Server instance. See Instructions for Content Tracker Reports New Install (page 2-13).

UNINSTALLING CONTENT TRACKER 6.5 OR EARLIER

1. Stop the web server.
2. Insert the Content Tracker 6.5 or earlier CD-ROM.
3. Launch the installation.

   win32:

   a. Select **Start—Run.**

   b. Click **Browse** and navigate to ContentTracker/win32 on the CD, double-click the **Setup.exe** file, then click **OK**.

   UNIX:

   a. Log in as the user who installed Content Server.

   b. **cd** to the ContentTracker/unix directory on the CD.

   c. Enter **`sh setup.sh`** from a shell window.

   The Install Setup screen is displayed.

4. Select the Content Server instance from which to uninstall Content Tracker, and click **OK**.

   The Content Tracker Install Setup screen is displayed, and the setup files (which are removed when uninstall is complete) are copied into the Content Server hierarchy.

5. Click **Continue**.

   The Install Type screen is displayed.

6. Click **Uninstall**.

   The Uninstall Confirmation screen is displayed.

7. Click **OK** to uninstall the component.

The Content Tracker Component Installer screen is displayed, and specific component files are uninstalled from the Content Server hierarchy.

Note: If an error message is displayed that indicates a certain file could not be deleted, note the name and location of the file, click **OK** to proceed, and remove the file manually after completing the uninstall.

8. Click **Finish** when prompted that the uninstall is complete.
9. Complete the uninstall by doing the following in the order listed:
   a. Stop and restart the web server.
   b. Stop and restart the Content Server master instance.
   c. Stop and restart the Content Server proxied instance.
10. If required, manually delete the file that the uninstaller was unable to delete.

Important: To manually delete the uninstalled file, it must first be unlocked. To do this, the Content Server and web server must be stopped and restarted. This is particularly important if you plan to install Content Tracker immediately following the uninstall.

Appendix

C

THIRD PARTY LICENSES

OVERVIEW

This appendix includes a description of the Third Party Licenses for all the third party products included with this product.

APACHE SOFTWARE LICENSE

```
* Unless required by applicable law or agreed to in writing, software
* distributed under the License is distributed on an "AS IS" BASIS,
 * WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, either express or implied.
 * See the License for the specific language governing permissions and
 * limitations under the License.
```

W3C® Software Notice and License

```
* Copyright © 1994-2000 World Wide Web Consortium,
* (Massachusetts Institute of Technology, Institut National de
* Recherche en Informatique et en Automatique, Keio University).
* All Rights Reserved.  http://www.w3.org/Consortium/Legal/
*
* This W3C work (including software, documents, or other related items) is
* being provided by the copyright holders under the following license. By
* obtaining, using and/or copying this work, you (the licensee) agree that
* you have read, understood, and will comply with the following terms and
* conditions:
*
* Permission to use, copy, modify, and distribute this software and its
* documentation, with or without modification, for any purpose and without
* fee or royalty is hereby granted, provided that you include the following
* on ALL copies of the software and documentation or portions thereof,
* including modifications, that you make:
*
*   1. The full text of this NOTICE in a location viewable to users of the
*      redistributed or derivative work.
*
*   2. Any pre-existing intellectual property disclaimers, notices, or terms
*      and conditions. If none exist, a short notice of the following form
*      (hypertext is preferred, text is permitted) should be used within the
*      body of any redistributed or derivative code: "Copyright ©
*      [$date-of-software] World Wide Web Consortium, (Massachusetts
*      Institute of Technology, Institut National de Recherche en
*      Informatique et en Automatique, Keio University). All Rights
*      Reserved. http://www.w3.org/Consortium/Legal/"
*
*   3. Notice of any changes or modifications to the W3C files, including the
*      date changes were made. (We recommend you provide URIs to the location
*      from which the code is derived.)
*
* THIS SOFTWARE AND DOCUMENTATION IS PROVIDED "AS IS," AND COPYRIGHT HOLDERS
* MAKE NO REPRESENTATIONS OR WARRANTIES, EXPRESS OR IMPLIED, INCLUDING BUT
* NOT LIMITED TO, WARRANTIES OF MERCHANTABILITY OR FITNESS FOR ANY PARTICULAR
* PURPOSE OR THAT THE USE OF THE SOFTWARE OR DOCUMENTATION WILL NOT INFRINGE
* ANY THIRD PARTY PATENTS, COPYRIGHTS, TRADEMARKS OR OTHER RIGHTS.
*
* COPYRIGHT HOLDERS WILL NOT BE LIABLE FOR ANY DIRECT, INDIRECT, SPECIAL OR
* CONSEQUENTIAL DAMAGES ARISING OUT OF ANY USE OF THE SOFTWARE OR
* DOCUMENTATION.
*
* The name and trademarks of copyright holders may NOT be used in advertising
* or publicity pertaining to the software without specific, written prior
* permission. Title to copyright in this software and any associated
* documentation will at all times remain with copyright holders.
*
```

ZLIB LICENSE

* zlib.h -- interface of the 'zlib' general purpose compression library
version 1.2.3, July 18th, 2005

Copyright (C) 1995-2005 Jean-loup Gailly and Mark Adler

This software is provided 'as-is', without any express or implied warranty. In no event will the authors be held liable for any damages arising from the use of this software.

Permission is granted to anyone to use this software for any purpose, including commercial applications, and to alter it and redistribute it freely, subject to the following restrictions:

1. The origin of this software must not be misrepresented; you must not claim that you wrote the original software. If you use this software in a product, an acknowledgment in the product documentation would be appreciated but is not required.
2. Altered source versions must be plainly marked as such, and must not be misrepresented as being the original software.
3. This notice may not be removed or altered from any source distribution.

Jean-loup Gailly jloup@gzip.org
Mark Adler madler@alumni.caltech.edu

General BSD License

Copyright (c) 1998, Regents of the University of California

All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

"Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

"Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

"Neither the name of the <ORGANIZATION> nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

GENERAL MIT LICENSE

Copyright (c) 1998, Regents of the Massachusetts Institute of Technology

Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the "Software"), to deal in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, sublicense, and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, subject to the following conditions:

The above copyright notice and this permission notice shall be included in all copies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

UNICODE LICENSE

UNICODE, INC. LICENSE AGREEMENT - DATA FILES AND SOFTWARE

Unicode Data Files include all data files under the directories http://www.unicode.org/Public/, http://www.unicode.org/reports/, and http://www.unicode.org/cldr/data/ . Unicode Software includes any source code published in the Unicode Standard or under the directories http://www.unicode.org/Public/, http://www.unicode.org/reports/, and http://www.unicode.org/cldr/data/.

NOTICE TO USER: Carefully read the following legal agreement. BY DOWNLOADING, INSTALLING, COPYING OR OTHERWISE USING UNICODE INC.'S DATA FILES ("DATA FILES"), AND/OR SOFTWARE ("SOFTWARE"), YOU UNEQUIVOCALLY ACCEPT, AND AGREE TO BE BOUND BY, ALL OF THE TERMS AND CONDITIONS OF THIS AGREEMENT. IF YOU DO NOT AGREE, DO NOT DOWNLOAD, INSTALL, COPY, DISTRIBUTE OR USE THE DATA FILES OR SOFTWARE.

COPYRIGHT AND PERMISSION NOTICE

Copyright © 1991-2006 Unicode, Inc. All rights reserved. Distributed under the Terms of Use in http://www.unicode.org/copyright.html.

Permission is hereby granted, free of charge, to any person obtaining a copy of the Unicode data files and any associated documentation (the "Data Files") or Unicode software and any associated documentation (the "Software") to deal in the Data Files or Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, and/or sell copies of the Data Files or Software, and to permit persons to whom the Data Files or Software are furnished to do so, provided that (a) the above copyright notice(s) and this permission notice appear with all copies of the Data Files or Software, (b) both the above copyright notice(s) and this permission notice appear in associated documentation, and (c) there is clear notice in each modified Data File or in the Software as well as in the documentation associated with the Data File(s) or Software that the data or software has been modified.

THE DATA FILES AND SOFTWARE ARE PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OF THIRD PARTY RIGHTS. IN NO EVENT SHALL THE COPYRIGHT HOLDER OR HOLDERS INCLUDED IN THIS NOTICE BE LIABLE FOR ANY CLAIM, OR ANY SPECIAL INDIRECT OR CONSEQUENTIAL DAMAGES, OR ANY DAMAGES WHATSOEVER RESULTING FROM LOSS OF USE, DATA OR PROFITS, WHETHER IN AN ACTION OF CONTRACT, NEGLIGENCE OR OTHER TORTIOUS ACTION, ARISING OUT OF OR IN CONNECTION WITH THE USE OR PERFORMANCE OF THE DATA FILES OR SOFTWARE.

Except as contained in this notice, the name of a copyright holder shall not be used in advertising or otherwise to promote the sale, use or other dealings in these Data Files or Software without prior written authorization of the copyright holder.

____Unicode and the Unicode logo are trademarks of Unicode, Inc., and may be registered in some jurisdictions. All other trademarks and registered trademarks mentioned herein are the property of their respective owners

MISCELLANEOUS ATTRIBUTIONS

Adobe, Acrobat, and the Acrobat Logo are registered trademarks of Adobe Systems Incorporated.

FAST Instream is a trademark of Fast Search and Transfer ASA.

HP-UX is a registered trademark of Hewlett-Packard Company.

IBM, Informix, and DB2 are registered trademarks of IBM Corporation.

Jaws PDF Library is a registered trademark of Global Graphics Software Ltd.

Kofax is a registered trademark, and Ascent and Ascent Capture are trademarks of Kofax Image Products.

Linux is a registered trademark of Linus Torvalds.

Mac is a registered trademark, and Safari is a trademark of Apple Computer, Inc.

Microsoft, Windows, and Internet Explorer are registered trademarks of Microsoft Corporation.

MrSID is property of LizardTech, Inc. It is protected by U.S. Patent No. 5,710,835. Foreign Patents Pending.

Oracle is a registered trademark of Oracle Corporation.

Portions Copyright © 1994-1997 LEAD Technologies, Inc. All rights reserved.

Portions Copyright © 1990-1998 Handmade Software, Inc. All rights reserved.

Portions Copyright © 1988, 1997 Aladdin Enterprises. All rights reserved.

Portions Copyright © 1997 Soft Horizons. All rights reserved.

Portions Copyright © 1995-1999 LizardTech, Inc. All rights reserved.

Red Hat is a registered trademark of Red Hat, Inc.

Sun is a registered trademark, and Sun ONE, Solaris, iPlanet and Java are trademarks of Sun Microsystems, Inc.

Sybase is a registered trademark of Sybase, Inc.

UNIX is a registered trademark of The Open Group.

Verity is a registered trademark of Autonomy Corporation plc

Index